Detailed Response of 11/03/06

1. Your letter states "Referring to claims 1,2,3,5,7 and 11, Kinsella discloses an input device (603) (i.e. trackball pointing device) to continuously detect biometrics for facilitating continuous authentication of the user's identification based on input from sensors attached to the device comprising (col. 3 lines 15-20): a computer mouse (603) (i.e. trackball pointing device), for providing a base with sensors that indicate different pressures applied to the base by a user (col. 18 lines 23-25) at different buttons 1,2,3;"

   The three buttons mentioned Kinsella (US# 6,914,517 - col. 18 lines 23-25) are switches as depicted schematically in Kinsella, Fig. 12. The pressures applied to the buttons are to activate a switch and do not measure different levels of pressures applied to the computer mouse. This application (10/660,542) describes pressure sensors that measures different levels of pressure as depicted in Fig. 8 of the application.

   Kinsella (US# 6,914,517), Kharon et al. (US# 6,487,662) and Mambakkam et al. (US# 200210073340) are all fingerprint based authentication devices. The current application (10/660,542) is based temporal detection of different pressures applied to the computer mouse. Neither Kinsella or Kharon patents sited in the letter mailed 11/03/06 refer to a the use of the pressures applied to a computer mouse to continuously detect the identity of the user.

   Mambakkam et al., in paragraph 31 states "The pressure sensor may have a resolution that is fine enough to obtain the biometric information, or an optical scanner such as a laser may be activated by the pressure sensor to scan the user's finger to obtain the biometric information . . ." This is only a passing comment to the use of pressure as a biometric and Mambakkam et al. makes only two other unrelated references to the use of finger pressure in the patent application. Mambakkam et al. does not stipulate a method for collecting pressure data or analyzing pressure data. Also, Mambakkam et al. does not make any mention of pressure or the use of pressure in the claims.

   The two other instances where Mambakkam et al. mentions pressure are both unrelated to the use of pressure as a biometric identifier are subsequently described. The first instance is at the end of the previously quoted sentence of paragraph 31, where finger pressure is used to activate the device. And second instance is in paragraph 52, where Mambakkam et al.'s device should be able to compensate for the differential pressure applied when a person has a finger cut. "The comparison may require that the match be within a certain threshold of an complete match, allowing for some differences in the biometric data, such as when the user has cut his finger or when a different amount of pressure is applied by the finger."

   In Matchett et al. (US# 5,229,764) col. 1, lines 63-68 & col. 2, lines 1-3, no mention of the pressures applied to a computer mouse is referenced. Matchett et. al's invention describes a generic analysis system, with out any specifics given to temporal biometric trait extraction from the pressure wave produced by a user on a computer mouse. Borza et al. (US# 5,991,431) uses the fingerprint as its sole biometric identifier using an imaging system. Borza does not mention of any alternate biometric device. In Brooks (US# 6,898,299) col. 1, lines 41-47, Brooks mentions several biometric characteristics used to identify people. The pressures applied to a computer mouse are not mentioned. Brooks identified the uniqueness of the patent in Brooks claim #1, col 58, lines 38-43 as an electric field unique to the individual. This application (10/660,542) similarly uses the pressures applied to a computer mouse as unique to the individual.

In Kinsella's patent, col. 11 lines 23-26, as shown above, Kinsella clarifies the additional biometric as being a precious gem. In Kinsella's patent, col. 16 lines 27-30, the precious gem is further clarified as being a diamond ("In other words, the feature detection sensor 544B reads a featureprint of the authentication article including a precious gem such as a diamond."). This is further evidence that Kinsella did not intend to use the pressures applied to a pointing device as a biometric and in this application.

2. In reference to Kinsella, your letter states
   a. "an authentication computer (612) (i.e. computer verification engine), for receiving and analyzing data from the sensor electronics for registration and continuous authentication, electrically connected to said sensor electronics module (col. 19 lines 11-57);"
   b. a registration module (614) (i.e. interface controller), for initially linking the user's identity to the user's biometric characteristics, totally embedded to said authentication computer (61 2) (i.e. computer verification engine) (col. 19 lines 8-24; see Figure 14);
   c. a biometric characteristics extractor, for extracting a set of biometric characteristics from the digitized signal (col. 19 lines 49-57);
   d. a software identity database, for linking the user identity to the user's biometric characteristics in the database (col. 19 lines 49-57; see Figure 14);
   e. a continuous authentication module, for continuously verifying that the identity of a user is authorized, algorithmically connected to said registration module, and totally embedded to said authentication computer (61 2) (i.e. computer verification engine) (col. 3 lines 15-20 and col. 20 lines 1-1 0);
   f. a biometrics correlation unit, for matching a new set of biometric characteristics with the biometric characteristics in the identity database (col. 19 lines 55-67); and an unauthorized user protocol, for changing the user's computer access (col. 11 lines 8-21 and col. 20 lines 15-67)."

These are analysis features common to most biometric identification devices. The component flow chart shown in Figure 5 and 6 of this application, shows those components specifically needed to process the pressures applied to a computer mouse for continuous identification. Design and algorithms may vary, but the concept is that the unique identifier, the pressures applied to a computer mouse, are processed to produce a continuous identification of the user. I do not believe Kinsella envisioned measuring the pressures applied to a computer mouse using the fingerprint sensor and circuitry or analyzing a pressure sensor signal using the Kinsella algorithms shown in figures 3, 4A, 4B, 4C or 5 of Kinsella's patent.

3. Your letter states "However, Kinsella did not explicitly disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse."

The uniqueness of this application is the biometric being identified, which is the pressure applied to a computer mouse over time. Kinsella used fingerprints. This application uses the different pressures applied to the computer mouse by a user over time. What Kinsella describes beyond the sensors is a system common to most identification systems. The difference occurs because fingerprint patterns are spatial in nature while the pressures applied to a computer mouse is temporal in nature. The system described in this application is specific for the continuous authentication of users based on the different levels of pressures applied to a computer mouse over time.

4. Your letter states
   a. "In the same field of endeavor of security system, Kharon et al. disclose an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse (col. 8 lines 48-65; see Figure 4).
   b. One ordinary skill in the art understands that an electrical sensor electronics module, for conditioning the analog signal so that it can be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. is desirable in the security system of Kinsella because Kinsella discloses the biometric data is used as an input to a computer mouse for authorizing to use a computer system (col. 4 lines 40-64) and Kharon et al. suggest a A/D converter converting the fingerprint input and verifying the data through a microcontroller 150 (col. 8 lines 48-65). Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to include an electrical sensor electronics module, for conditioning the analog signal so that it carl be converted into a digital signal, electrically connected to said computer mouse of Kharon et al. in the security computer system of Kinsella with the motivation for doing so would allow the biometric data to convert into digital data in order to compare."

The analog-to-digital converter mentioned by Kharon et al. (US# 6,487,662 - col. 8 lines 48-65; see Figure 4) is a common device. Kharon is using it to convert various image intensity levels from an analog to digital form. Again, Kharon is converting fingerprint images and not pressures applied to a computer mouse over time. In this application, the different pressures applied to the computer mouse is converted from an analog to digital signal so that the digital computer can process it.

5. Your letter states
   a. "In the same field of endeavor of authentication system, Mambakkam et al. disclose a comparison of different biometric pressures authenticating the computer system (paragraphs 12 and 52).
   b. One ordinary skill in the art understands that a comparison of different biometric pressures authenticating the computer system of Mambakkam et al. is desirable in the authentication system of Kinsella in view of Kharon et al. because Kinsella, Kharon et al. and Mambakkam et al. teach the used of biometric for authenticating a computer system, and Mambakkam et al. teach further disclose the comparison of different biometric pressures at a certain threshold order to authenticate the computer system."

Mambakkam et al. does not mention pressure or the measurement of pressure in paragraph 12 as shown in the subsequent quote from Mambakkam et al. "[0012] Biometric devices have been used to secure computers such as PC's. For example, a computer mouse can have a fingerprint reader that scans the user's fingerprint to use for authentication in place of a password. However, the authentication software routines typically reside on the PC or even on a network server. If the fingerprint-reading mouse were moved to a different PC, authentication would not be possible as that PC would not necessarily have the authentication software installed, not would it have a reference fingerprint for the same user. Thus PC-based biometric authentication limits the user to specially-configured PC's or networks of such PC's."

Mambakkam et al., in paragraph 31 states "The pressure sensor may have a resolution that is fine enough to obtain the biometric information, or an optical scanner such as a laser may be activated by the pressure sensor to scan the user's finger to obtain the biometric information . . ." This is only a passing comment to the use of pressure as a biometric and Mambakkam et al. makes only two other unrelated references to the use of finger pressure in the patent application. Mambakkam et al. does not stipulate a method for collecting pressure data or analyzing the data. Also, Mambakkam et al. does not make any mention of pressure or the use of pressure as a biometric identifier in the subsequent claims of the application.

The two other instances where Mambakkam et al. mentions pressure are both unrelated to the use of pressure as a biometric identifier are described. First, at the end of the previously quoted sentence of paragraph 31, where finger pressure is used to activate the device. And second, in paragraph 52, where Mambakkam et al.'s device should be able to compensate for the differential pressure applied when a person has a finger cut. "The comparison may require that the match be within a certain threshold of an complete match, allowing for some differences in the biometric data, such as when the user has cut his finger or when a different amount of pressure is applied by the finger." Except for the passing comment about pressure as a biometric, there is no evidence within the application of Mambakkam et al. that pressure played any substantive role as a biometric identifier.

6. Your letter states:
"Referring to claim 4, Kinsella in view of Kharon et al. and Mambakkam et al. disclose the input device to continuously detect biometrics in accordance with claim 1, Kinsella discloses wherein said means for receiving and analyzing data from the sensor electronics for registration and continuous authentication comprises an authentication computer (col. 12 lines 8-19; see Figure 5)."

From Kinsella, col. 12, lines 7-19.
"FIG. 5 shows exemplary hardware/software components in a system 400. The system 400 generally incorporates an array of fingerprint sensors 70A through 70C shown in FIG. lB to provide controllable access to a secured application executed from an information processor 405 using Internet 410 in accordance with one aspect of the invention. An individual may use a first computer, such as an IBM compatible computer 415A, 415B, or 415C, to access over a computer network, such as the Internet 410, the secured application from the information processor 405 that preferably services multiple first authorized users. Those skilled in the art will appreciate that other computer networks can be readily substituted for the Internet 410."

Although there is mention of "authentication", there in no mention of an "input device to continuously detect biometrics" or "continuous authentication" as in this application. Using pressure as a biometric is also not mentioned.

7. Your letter states:
   "Referring to claim 13, Kinsella in view of Kharon et al. and Mambakkam et al. disclose the input device to continuously detect biometrics as claims 1 and 11, claim 13 is equivalent to that of claims 1 and 11 addressed above, incorporated herein. Therefore, claim 13 is rejected for same reasons given with respected to claims 1 and 11."

   Kinsella, Kharon et al. and Mambakkam et al. mentioned several biometric identifiers in col. 1, lines 56-58, but not the pressures applied to a computer mouse. It is unlikely, that Kinsella, Kharon et al. and Mambakkam et al.envisioned the use of the pressures applied to a computer mouse as a biometric since it had not been invented yet. Also the specialized schematics for a pressure sensor are missing from Kinsella's, Kharon et al.'s and Mambakkam et al's. patent. It is unlikely, that Kinsella, Kharon et al. and Mambakkam et al. fingerprint biometric identification system which uses fingerprint images would work with a temporal signal like that of a pressure sensor shown in figure 5 of this application. In Brooks (US# 6,898,299) in claim #1, col 58, lines 38-43 as an electric field unique to the individual. This application (10/660,542) similarly uses the pressures applied to a computer mouse as unique to the individual. The same reason the Brooks patent was granted, uniqueness of biometric, is precedence for this application to be granted.